【公表予定】
資　料　5

サイバーセキュリティ対策・内部不正防止対策

第９回営業秘密官民フォーラム

2023年6月28日

独立行政法人情報処理推進機構
セキュリティセンター長
高柳 大輔

ご説明内容

- 「情報セキュリティの10大脅威2023」とIPAの関連活動
- IPAの内部不正対策啓発活動
  「組織における内部不正防止ガイドライン」
  「企業における内部不正防止体制に関する実態調査」

情報セキュリティ10大脅威 2023 脅威ランキング

https://www.ipa.go.jp/security/vuln/10threats2023.html

・2022年に発生した情報セキュリティ事案を専門家投票によりランクづけ

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐欺	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭被害	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロディ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不正請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

IPAが脅威候補を選出し、専門家約200名からなる「10大脅威選考会」が投票

内部不正対策啓発に係るIPAの取り組み

1.「組織における内部不正防止ガイドライン」第5版改訂(2022年4月)

・内部不正防止の重要性や対策の体制、 関連する法律などの概要を説明
・「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の10の観点のもと、合計33項目の具体的な対策を示す

https://www.ipa.go.jp/security/guide/insider.html

2. 企業の内部不正防止体制に関する実態調査（2023年4月）

・内部不正による情報漏えいについて、企業の課題認識、対策状況、マネジメント体制等の実態を調査
・企業アンケート調査により1,179件の回答を集計・分析

https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

内部不正～最近の事例

＜転職者による情報漏えいの事例＞ A寿司チェーン社長、転職先に営業秘密持出し

- A寿司チェーン元社長は、2014年～2017年B同業他社の取締役、その後、B同グループ会社の社長
- 2020年10月　B社の顧客名簿や各店舗仕入れ値等のデータ持ち出し(アクセス権を持つ元部下メール)
- 2020年11月　A社顧問、2021年2月　A社社長就任
- 2023年5月 「懲役3年、執行猶予4年、罰金200万円」判決（東京地裁）

→退職者等に向けた対策（外部送信メールのチェック、秘密保持義務や競業避止義務等）？

＜保守委託事業者による顧客情報の不正利用事例＞ システム保守委託先の社員が不正利用

- 2021年3月　証券会社M社のシステムの保守を委託されていた企業S社の元従業員が、証券会社の顧客情報を不正に取得、使用したとして逮捕
- M社本番環境から顧客情報ファイルを抽出して私用メールアドレスへ送付
  顧客12人のID、パスワード、暗証番号等を不正利用し、有価証券の売却や現金の不正出金
  被害総額は約2億円弱
- 2022年１月「懲役4年6月」の実刑判決（東京地裁）

→事案後、M社は保守管理業務の監視強化、S社は情報セキュリティー研修強化等の再発防止策を実施

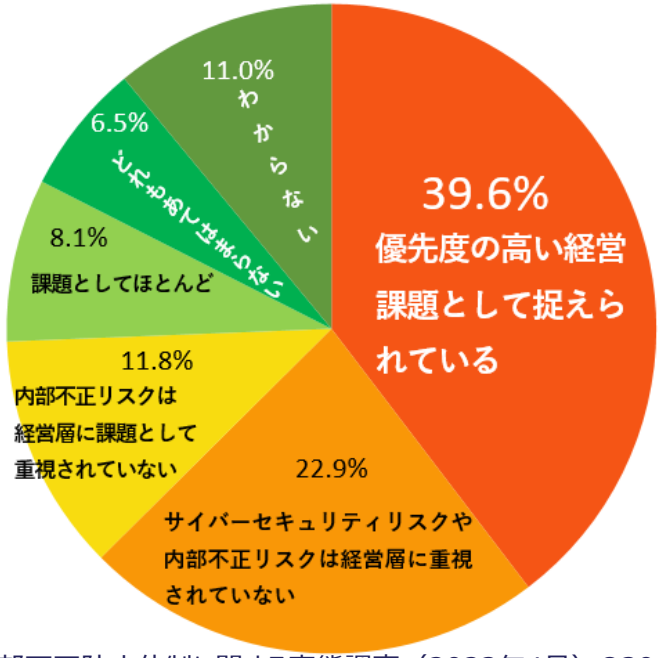
（実態調査）内部不正対策に取り組む経営層の姿勢

組織の状況

経営層が内部不正リスクを優先経営課題とした率は約4割

- 内部不正は、従業員のモラルやリテラシーに起因する事案だけではない。
- **重要技術情報を狙う外部の関与するケース**も、事業リスクの低減の観点から大きな経営課題。

内部不正リスクを経営課題として捉えていますか



経営層に望まれること

- 重要情報漏えいの事業リスクを喫緊の**問題と認識**
- 内部不正防止について**リーダーシップ**を発揮
- 内部不正防止取組み推進の方針を**情報発信**
- **コンプライアンス重視**の徹底

企業の内部不正防止体制に関する実態調査（2023年4月）Q30を基に再構成

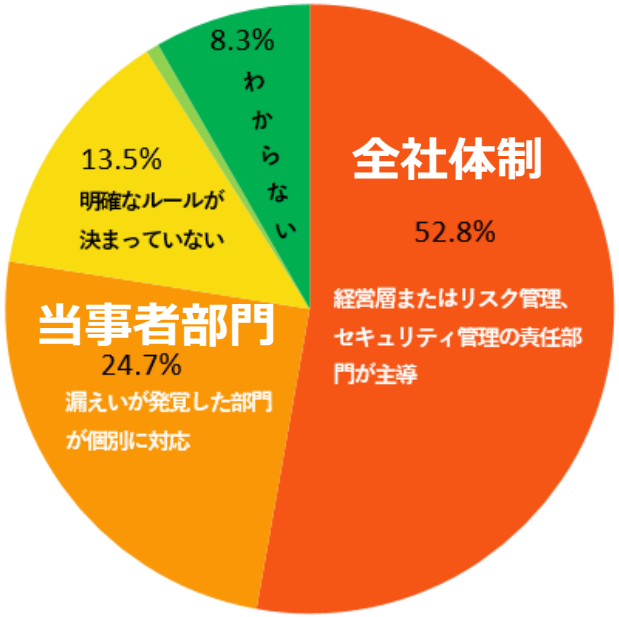
（実態調査）内部不正対策に取り組む組織的体制

組織の状況

内部不正対策を全社体制で行っているのは全体の5割のみ

- **情報漏洩は、情報取扱ポリシーの弱いところで発生する**おそれ。
- 守るべき情報資産・IT資産が、海外子会社、グループ子会社、委託先事業などに広範囲にわたる場合は、それに応じて、**内部不正対策も全社的なガバナンス下での対応**が重要。

重要情報が漏えいした時に対応する部門



各部門が連携した全社的な対応が重要

経営者、コンプライアンス部門

-基本方針の策定

情報取扱ポリシーの作成
内部不正に係る就業規則の整備

-資産の把握、対応体制の整備

重要資産を把握、重要度に応じた情報管理者を定める

-人的管理およびコンプライアンス教育の徹底

秘密保持義務、競業避止義務の有無や内容の確認
誓約書取得（第三者の秘密情報を持ち出していないなど）

情報システム／セキュリティ管理部門

-重要情報の利用者ID、アクセス権の管理

-システム操作履歴の監視

不自然なデータアクセスの通知、外部送信メールのチェック、PCやネットワーク等のログの記録・保存とその周知など

企業の内部不正防止体制に関する実態調査（2023年4月）Q10を基に再構成

IPA Better Life with IT

お問い合わせ・ご相談先

＜内部不正防止対策＞
セキュリティセンター
isec-info@ipa.go.jp

＜標的型サイバー攻撃＞
サイバーレスキュー隊（J-CRAT）
https://www.ipa.go.jp/security/J-CRAT/